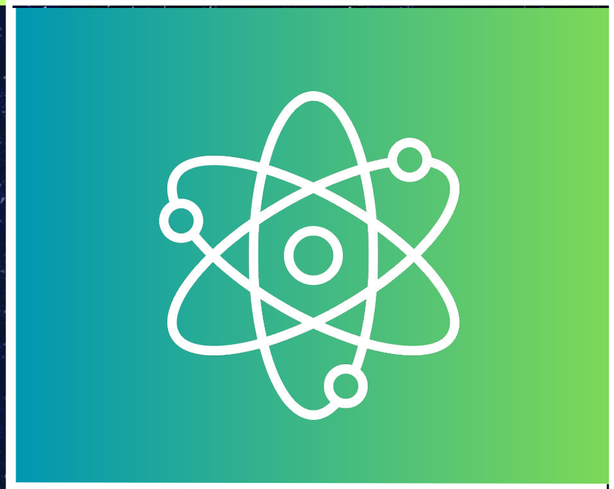
Quantum Cryptography

Security guaranteed by Physics?



Carter Chapman & Flor Nardone

Table Of Contents

Classical Cryptography

Symmetric vs Asymmetric Cryptography

Core Ideas

QKD (BB84 Protocol) and QBER

Eavesdropping

Eavesdropper concept, Intercept-Resend, Entangled Probe

Applications

Technical Challenges with QKD, BB84 implementation, Future

Classical Encryption

Two main types of classical encryption:

Symmetric Encryption

Asymmetric Encryption

Why is classical encryption important in this presentation if our topic is quantum cryptography?

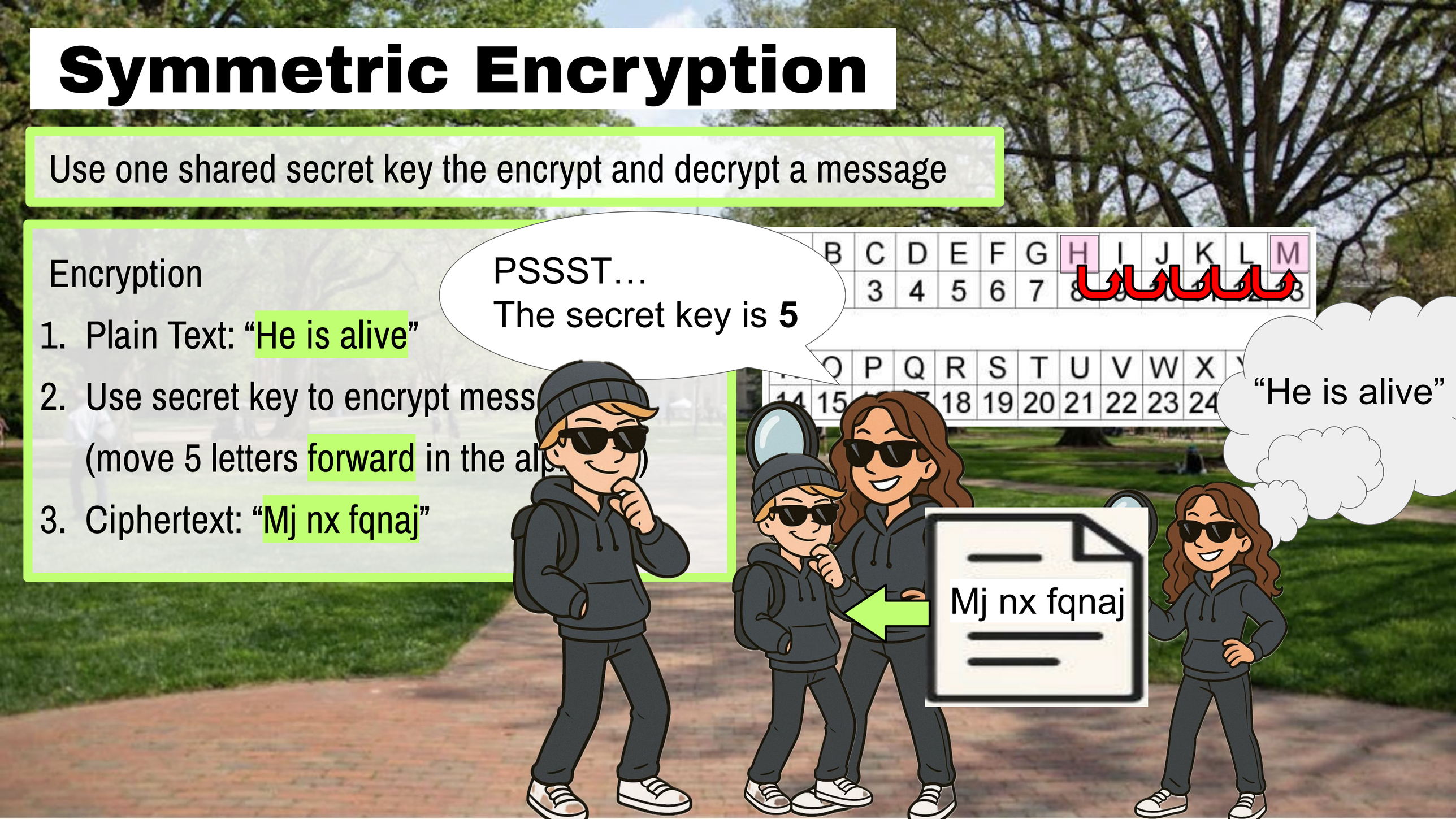
- Quantum cryptography (QKD specifically) solves the key distribution problem that plagues symmetric encryption
- QKD does not encrypt your data (it only generates and distributes secret keys)
- QKD is a complement to classical cryptography, not a replacement

Symmetric Encryption

Use one shared secret key the encrypt and decrypt a message

Encryption

1. Plain Text: “He is alive”
2. Use secret key to encrypt mess
   (move 5 letters forward in the al
3. Ciphertext: “Mj nx fqnaj”

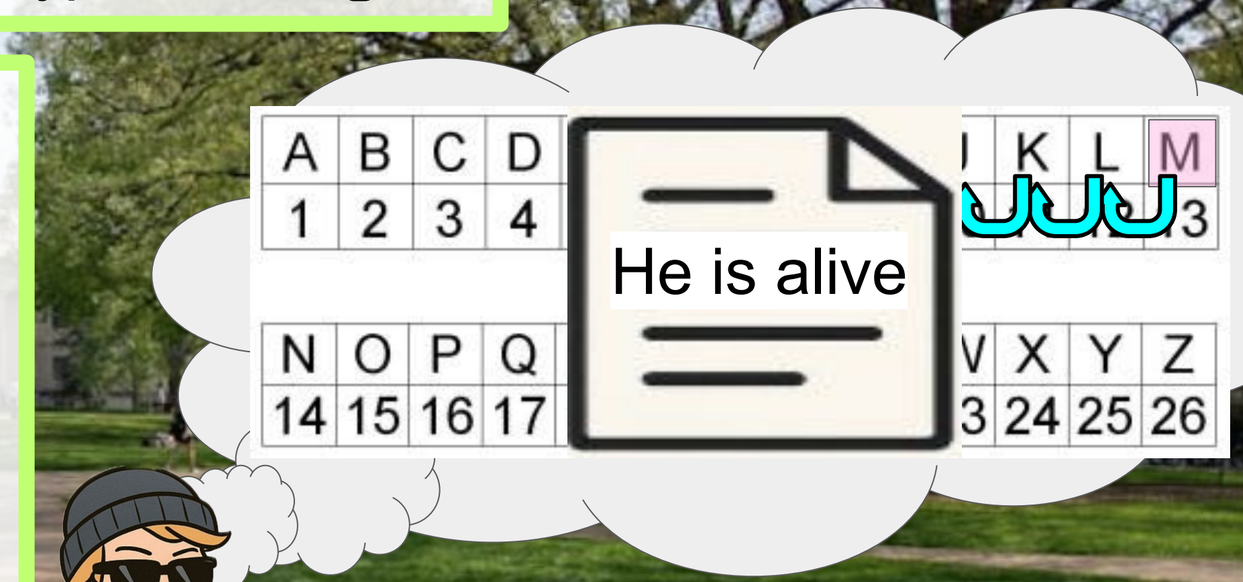


Symmetric Encryption

Use one shared secret key the encrypt and decrypt a message

Decryption (Reverse the SAME Process)

1. Ciphertext: “Mj nx fqnaj”
2. Use secret key to encrypt message: 5
   (move 5 letters backwards in the alphabet)
3. Plain Text: “He is alive”



Symmetric Encryption

Use one shared secret key the encrypt and decrypt a message

AES (Advanced Encryption Standard):

- modern day standard for symmetric encryption
- Function that has the secret key as a parameter:

  Encryption: Ciphertext = AES_Encrypt(Plaintext, Secret Key)

  Decryption: Message = AES_Decrypt(Ciphertext, Secret Key)
- Uses substitutions, permutations and mixing based on the secret key

Main Problem with Symmetric Encryption is: Key Distribution

- How do I get my secret key to Carter while ensuring no one overhears?
- Symmetric encryption is only as secure as the method by which you share and store the secret key

Without knowledge of the secret key, AES can only be attacked via brute force

- Classical computers are estimated to take ≈ 10^18 years (≈7 orders of magnitude larger than the age of the universe) to crack AES-128 encryption
- Quantum computers Grover's algorithm effectively halve the security strength (AES-128 ⟶ 64-bit effective security, AES-256 ⟶ 128-bit effective security), but this still remains computationally infeasible
  - Therefore it is Quantum Resistant

Asymmetric Encryption

Uses a key pair (public + private): anyone can encrypt with the public key, but only the private key holder can decrypt

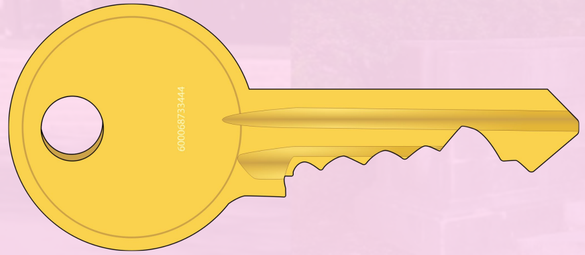
Step **1**: Encrypt data with intended receiver's public key

Step **2**: Send encrypted file

Step **3**: Receiver decrypts file using his private key

c Key

Private Key



Asymmetric Encryption

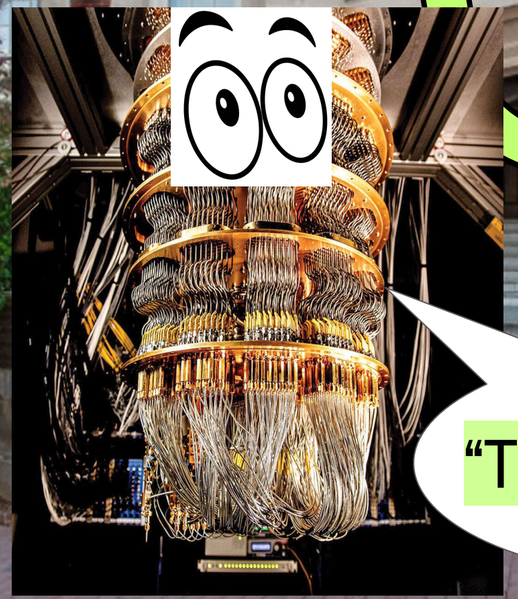
Uses a key pair (public + private): anyone can encrypt with the public key, but only the private key holder can decrypt

Making the Key Pairs:

- Based on mathematical algorithms called “one-way functions”
  - Easy to do but hard to reverse
- Reliant on the existence of a “really hard math problem”
  - Common “one-way” functions/algorithms used are RSA and ECC

Attack Threats:

- Secure against classical computers BUT vulnerable to quantum computers
- Quantum computers use superposition (qubits = 0 AND 1 simultaneously) to evaluate many possibilities at once
- Shor's algorithm exploits this to solve the underlying math problems exponentially faster
- What would take a classical computer millions of years, a quantum computer (with sufficient qubits) is estimated to crack in a couple of hours



Easy

Hard

“This looks easy”

Post-Quantum Cryptography

What is this?

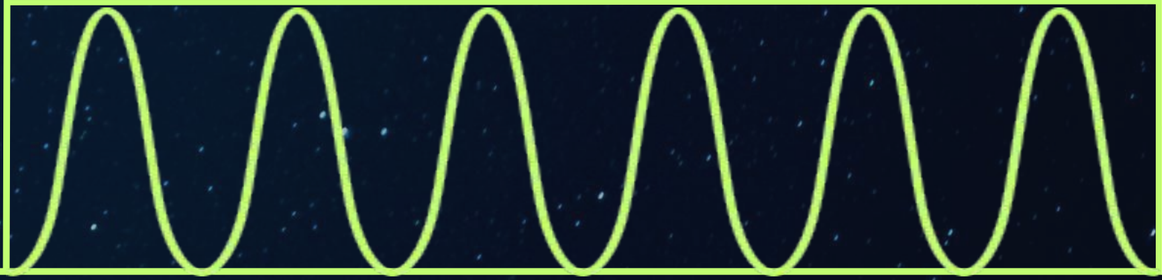
- New asymmetric encryption algorithms designed to resist both classical AND quantum computer attacks
- Based on different math problems where quantum computers provide no significant advantage (lattice-based, code-based, etc.)
- Still just a “really hard math problem” that is hard for even a quantum computer to solve

Advantages:

- Is deployable on current computers and networks
- no new hardware required

Limitation:

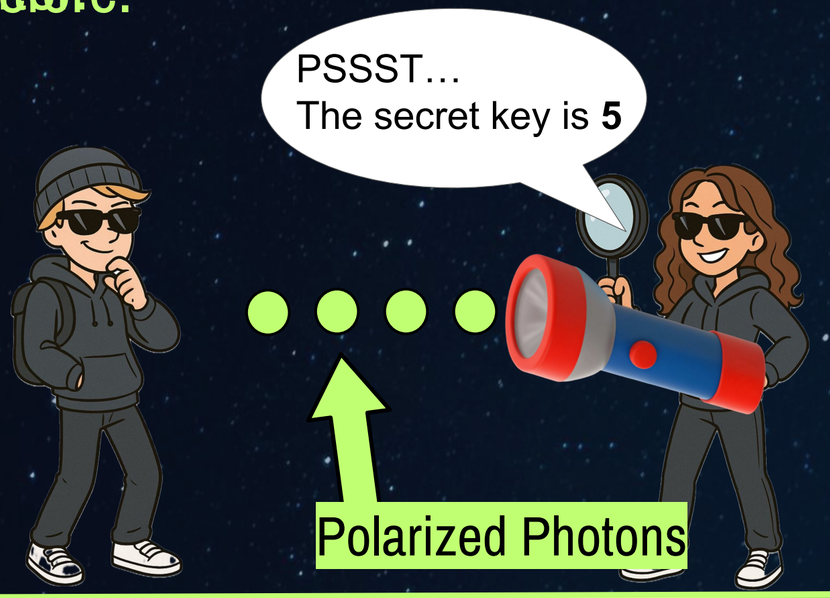
- Still relies on mathematical assumptions that could theoretically be broken by future algorithms



Intro to QKD

Symmetric Encryption, but better

Before:

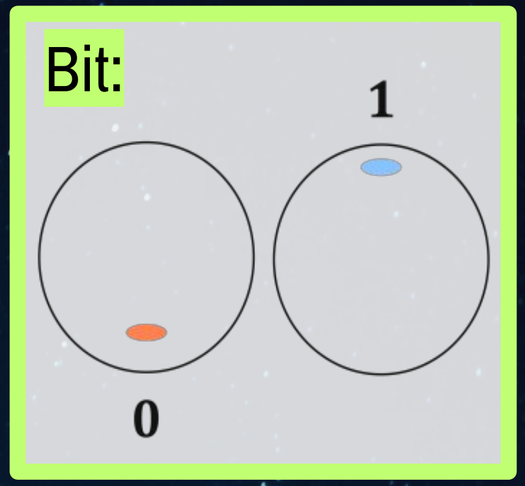


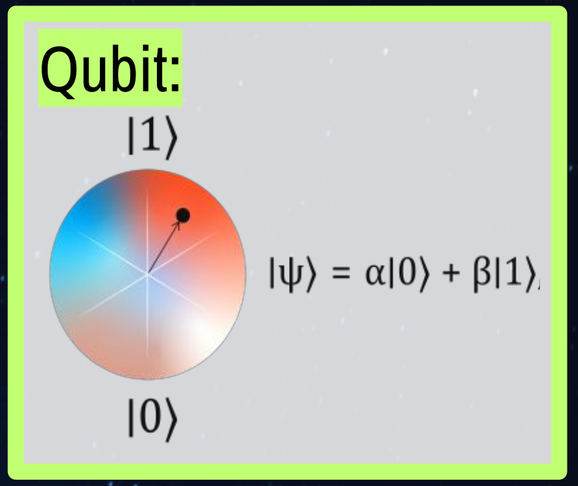
Quantum Key Distribution (QKD):

- A method by which we can create and share the “secret key” which we can later use for classical symmetric encryption
  - creates secret key we can later use to run AES
- A quantum solution to the key distribution problem
  - solves key distribution problem using the laws of physics instead of math (unlike asymmetric encryption)

Qubits and Quantum Information

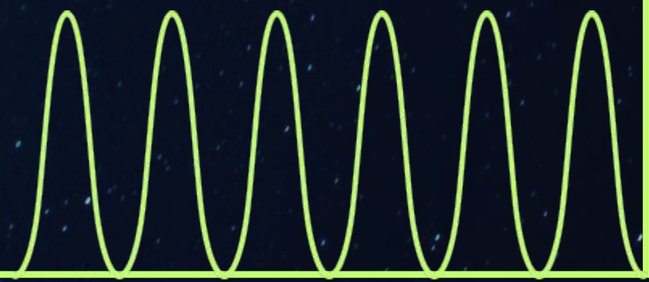
- Classical Bits - Have definite values of 0 or 1
- Qubit - Fundamental unit of Quantum Information
  - Qubits can exist in a superposition of states
  - Measurement collapses the state to either a 0 or 1
  - Unknown qubit state cannot be copied





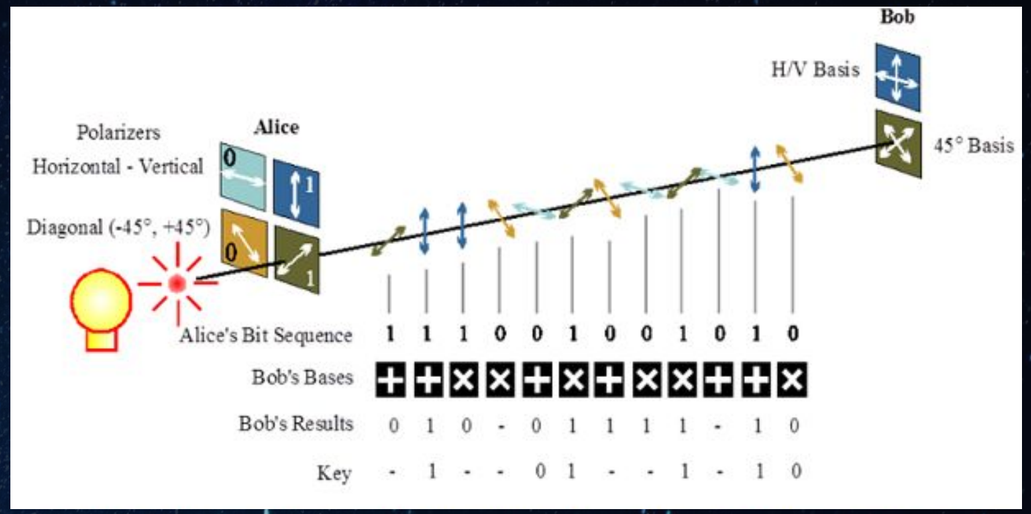
$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad |\alpha|^2 + |\beta|^2 = 1$$

Qubits should be treated and thought about just like wave functions



BB84 Protocol

- BB84 is a QKD protocol invented in 1984 by Charles Bennett and Gilles Brassard [3]
- Sender prepares quantum states, and the recipient performs measurements
- Qubits are individual particles (electrons, molecules, photons) with discrete quantum states (spin, polarization etc)
- Traditionally photons are sent via fiber optic cables, where sender and receiver compare photon orientations
- Particles can also be used but are less ideal because it is more difficult to control their path in free space



Polarized photons example for BB84

BB84 Protocol

General Pipeline:

1. Sender randomly prepares spin ½ particles in either X or Z basis, sends to recipient
2. Recipient measures in a random basis and records value
3. Repeat for multiple particles
4. After initial exchanges we publicly reveal which bases we sent/measure in
5. Drop all bases where we disagreed
6. Reveal a select amount of bits to confirm an eavesdropper was not present
7. Drop revealed bits and establish a secret (sifted) key

$$|\uparrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle + |\downarrow_z\rangle), \quad |\downarrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle - |\downarrow_z\rangle)$$

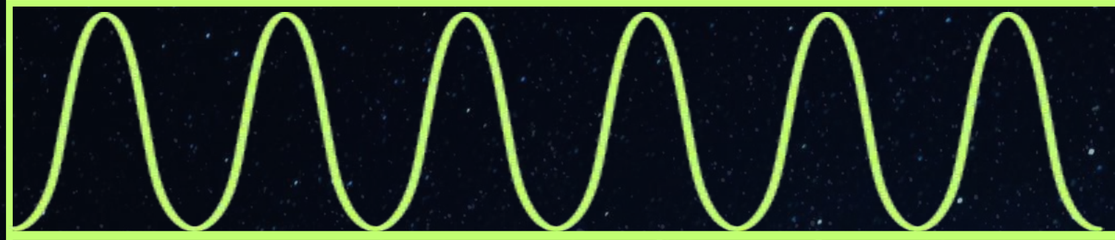
Assumptions:

Spin	Logical Bit
$\|\uparrow x\rangle$	1
$\|\uparrow z\rangle$	1
$\|\downarrow x\rangle$	0
$\|\downarrow z\rangle$	0

For this example:

	X
	Z
	↑
	↓

	1	2	3	4	5	6
C Bases	Z	Z	X	X	X	Z
C Spin	$\|\downarrow z\rangle$	$\|\downarrow z\rangle$	$\|\uparrow x\rangle$	$\|\downarrow x\rangle$	$\|\uparrow x\rangle$	$\|\uparrow z\rangle$
C Bit	0	0	1	0	1	1
F Bases	X	Z	X	X	Z	Z
F Spin	$\|\downarrow x\rangle$	$\|\downarrow z\rangle$	$\|\uparrow x\rangle$	$\|\downarrow x\rangle$	$\|\uparrow z\rangle$	$\|\uparrow z\rangle$
F Bit	0	0	1	0	1	1
Correct	NO	YES	YES	YES	NO	YES
Shared Bits		0	1	0		1
Bit Reveal		0	1			
Secret Key				0		1



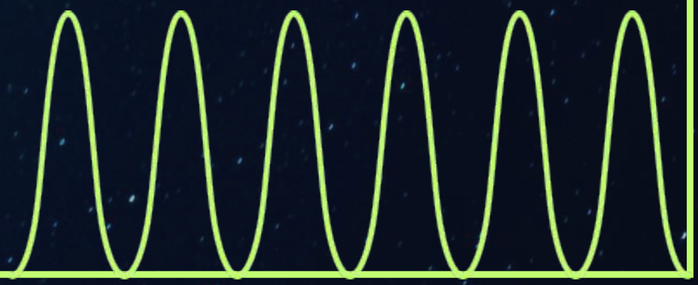
QBER

- After sender and recipient have thrown out mismatching bases, they can share the results of a portion of their qubit values (0 or 1)
- If there are too many disagreements then they throw out the old key and start over again
- Metric of success is the Quantum Bit Error Rate (QBER)
- QBER < 11% is considered a safe key, (many outside variables can affect QBER will discuss later) [4]

$$QBER = \frac{\text{Number of mismatched bits}}{\text{Total number of bits compared}}$$

Eavesdropping

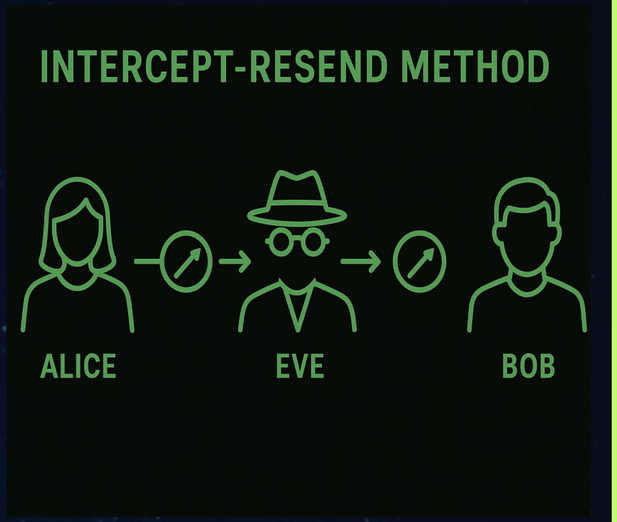
- Eavesdropping refers to the act of an unauthorized third party attempting to intercept a transmission or in our case listen in on QKD
- One of the biggest advantages to Quantum Cryptography is that the quantum state is perturbed when an eavesdropper makes a measurement. Easily alerting the sender and intended recipient if an eavesdropper is present
- We will discuss two methods of eavesdropping, the Intercept-Resend Method, and the Entangling Probe Method



Intercept and Resend Method

In this case the eavesdropper:

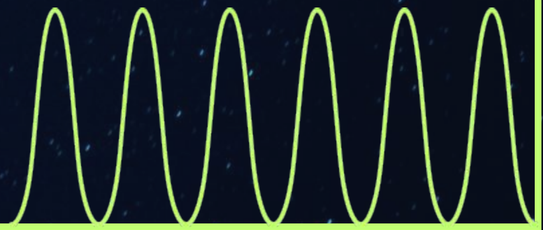
1. Positions themself in between the sender and recipient, measuring the incoming particles in random basis of their choice (either X, or Z)
2. After the eavesdropper measures they send another particle to the recipient that depends on their measurement



Two outcomes arise:

1. Eavesdropper chooses the correct basis with 50% probability and forwards the correct state, introducing no error
2. Eavesdropper chooses the wrong basis, collapses the wave function, and forwards the incorrect state. Recipient now has a 50% chance of measuring the correct bit

$$QBER = 25\% \text{ (intercept–resend, random basis)}$$



Entangled Probe Eavesdropping Method

- The eavesdropper uses a unitary interaction to entangle a “probe” with the exchanged qubit between the sender and recipient
- A unitary interaction entangles two quantum systems without measuring either of them (idealistic interaction). An example of this is a controlled-not (C-NOT) gate (small quantum circuit)
- Probe carries information about the qubit without destroying the overall quantum state [5]
- The probe has an initial state, then interacts with the particle and takes on another state depending on the spin of the particle

$$|\uparrow_z\rangle \otimes |e_0\rangle) = |\uparrow_z\rangle \otimes |e_\uparrow\rangle$$
$$|\downarrow_z\rangle \otimes |e_0\rangle) = |\downarrow_z\rangle \otimes |e_\downarrow\rangle$$

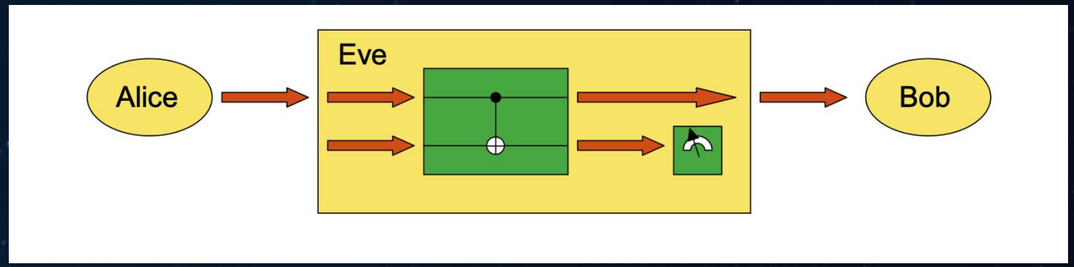


Figure 1: Example of Eavesdropper (Eve) using a C-NOT gate to entangle and probe with the signal photon [5]

Entangled Probe Eavesdropping Method

- Using the same interaction show previously, assume the sender prepares a particle with spin
  - Text

$$|\uparrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle + |\downarrow_z\rangle)$$

- The Z states become coupled with the probe states as shown previously and rewriting the equation yields

$$|\uparrow_z\rangle = \frac{1}{\sqrt{2}}(|\uparrow_x\rangle + |\downarrow_x\rangle), \quad |\downarrow_z\rangle = \frac{1}{\sqrt{2}}(|\uparrow_x\rangle - |\downarrow_x\rangle),$$

$$\frac{1}{2}\Big(|\uparrow_x\rangle \otimes (|e_\uparrow\rangle + |e_\downarrow\rangle) + |\downarrow_x\rangle \otimes (|e_\uparrow\rangle - |e_\downarrow\rangle)\Big).$$

Entangled Probe Eavesdropping Method

- Now the probability the recipient measures the incorrect bit is given below

$$P_{\text{err}|X} = \frac{1}{4}\left\| |e_{\uparrow}\rangle - |e_{\downarrow}\rangle \right\|^2 = \frac{1}{4}\left(2 - 2\,\text{Re}\langle e_{\uparrow}|e_{\downarrow}\rangle\right) = \frac{1}{2}\left(1 - \text{Re}\langle e_{\uparrow}|e_{\downarrow}\rangle\right)$$

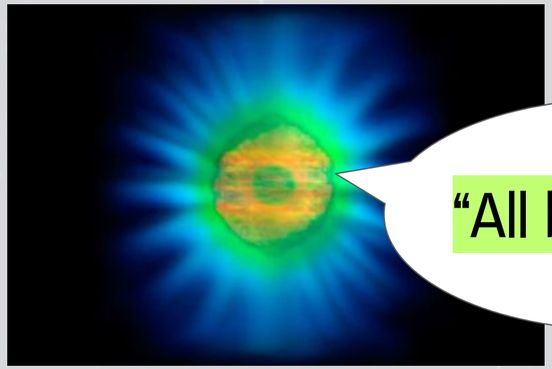
- Highlights the information-disturbance trade-off. If the eavesdropper probe states are orthogonal, then they gain the most information, but the state is more disturbed (high QBER). If the states are identical then there is no disturbance but the eavesdropper won't gain any information
- This tradeoff captures the elegance of QKD: gaining information means causing disturbance, and that's exactly what keeps the protocol secure

Technical Challenges

Quantum cryptography relies on real physics but faces practical challenges.

- QKD assumes reliable single-photon sources, yet most systems use laser pulses that can carry multiple photons, creating potential security risks.
- Over long distances, photons can be lost or have their polarization altered in fibers or free space.
- Requires the adoption of new hardware
- Massive particles are hard to transmit and measure individually, making them impractical as qubits.

Assumes:



Real Word BB84

- In “Experimental Side Channel Analysis of BB84 QKD Source” [6] the authors use four non-identical laser diodes to create pulses with four different polarization states
- Results showed imperfections due to slight rotations experienced while traveling through optical fibers
- Variations in wavelength and pulse width of the lasers create non-ideal quantum states
- Authors discuss methods to reduce errors in photon generation such as bandwidth filters and improved cooling for less uncertainty in pulse width and wavelength

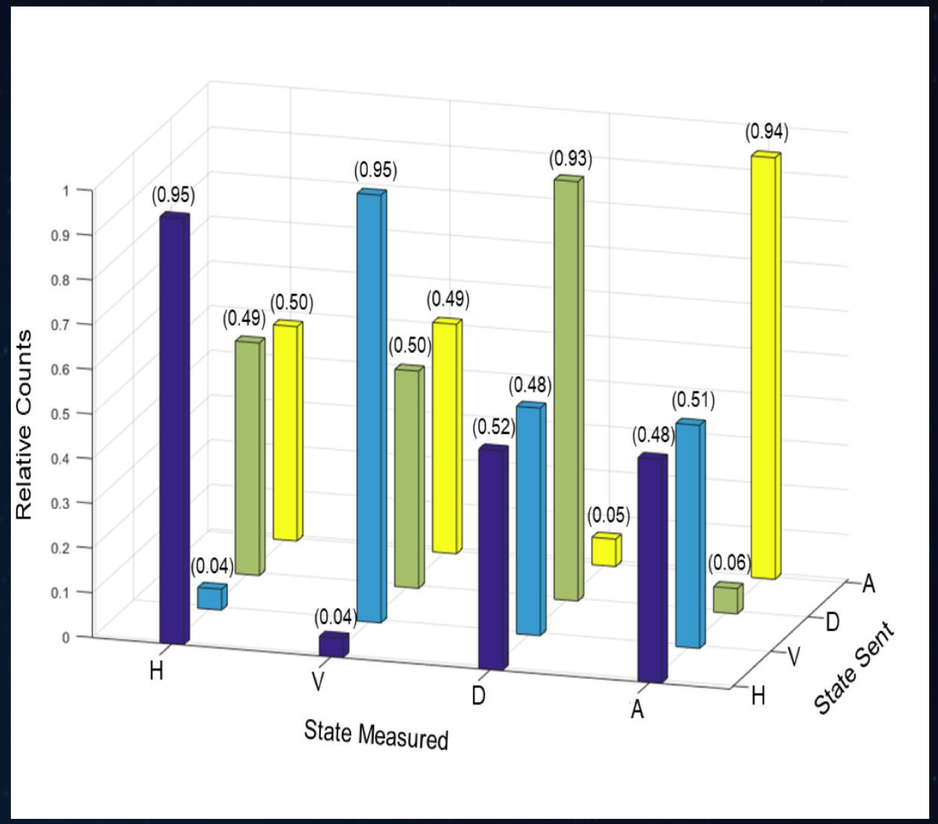


Figure 1: Histogram showing state sent vs state measure for each of the polarization states [6]

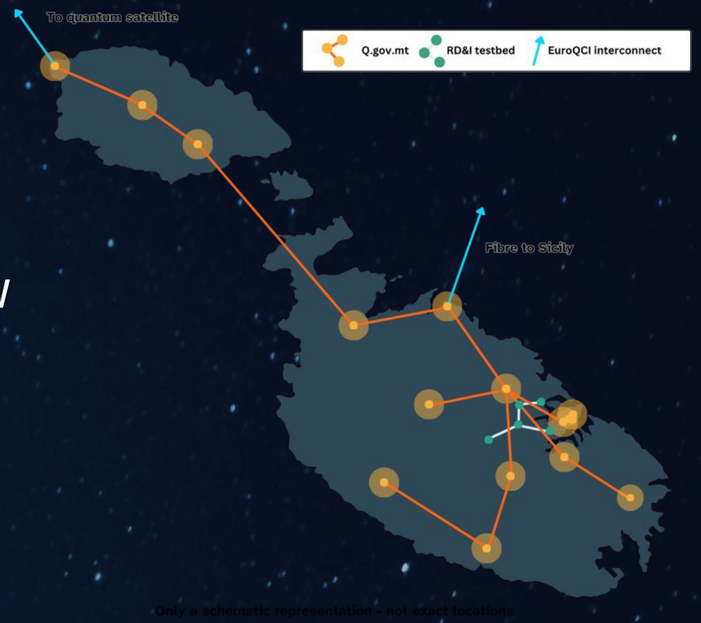
Future?

Continuous Variable QKD:

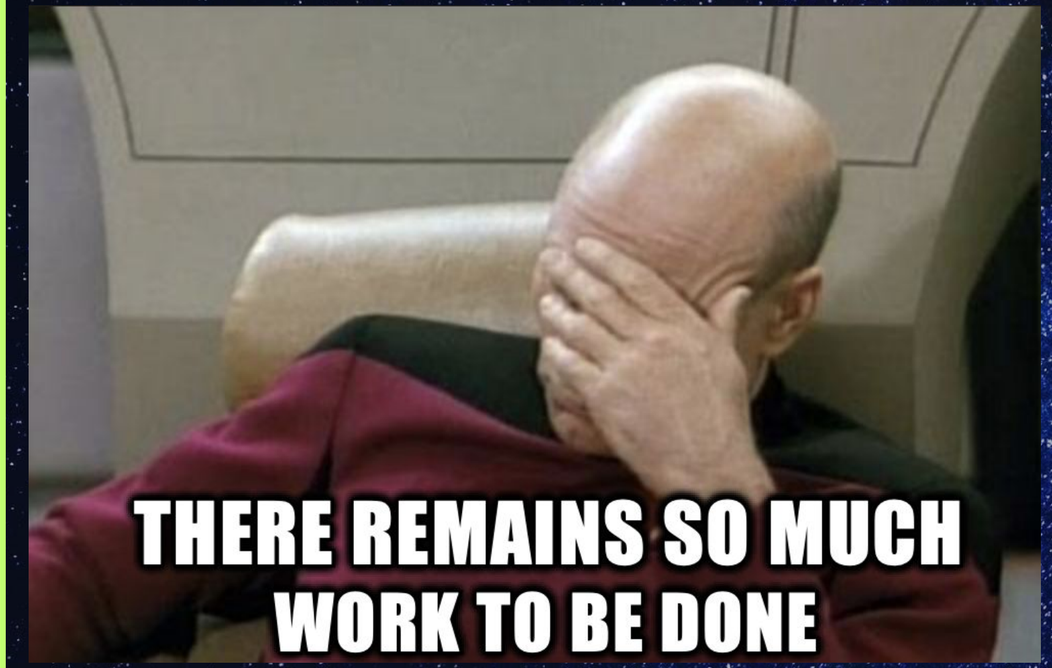
- CV-QKD encodes qubits in the amplitude and phase difference of signals, as opposed to discrete quantum states. More practical for communication without optic fibers [7]

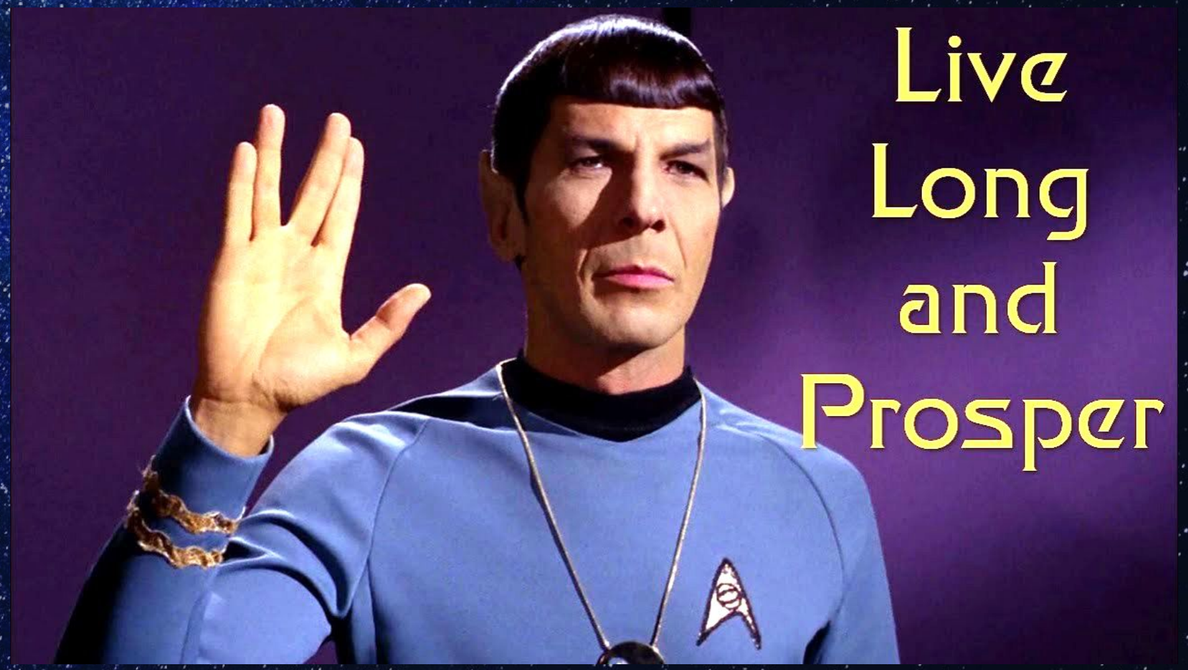
QKD Virtual Networks:

- Implement logical/virtual connections on top of physical QKD links to allow flexible key distribution [8]
- Help increase efficiency by enabling key forwarding, slicing, and aggregation across multiple physical links
- Introduce risks similar to classical networks: the logical layer relies on trusted nodes, so misconfiguration or compromise can open the network to traditional cyberattacks, evelves remain quantum-secure when endpoints are trusted



The End (for now)





Works Cited

Pictures:

Eavesdropper Picture - Eavesdropping Snoops - The average person's guide to stopping them

Qubits- Quantum 101 - What is a Qubit?. Quantum Cryptography Blog - QNu Labs

Black key - Key Icon. Transparent Key.PNG Images & Vector - FreeIconsPNG

Gold key - Key Png Image Transparent HQ PNG Download | FreePNGimg

Folded laundry - Stack of folded clothes pile of clean shirts isolated on white transparent background | Premium AI-generated image

Messy laundry - Dirty Laundry Pile Images – Browse 33,714 Stock Photos, Vectors, and Video | Adobe Stock

Lock - Lock - Free security icons

Quantum Computer- Quantum computers take key step toward curbing errors | Science | AAAS

BB84 - Confluence Mobile - GÉANT federated confluence

Malta QKD - prism-euroqci.eu

Some images were created using chatGPT:

OpenAI. (2025). ChatGPT-5.1 Thinking [Large language model]. https://chat.openai.com/chat

Information:

[1]Practical Networking. “Encryption - Symmetric Encryption vs Asymmetric Encryption - Cryptography - Practical TLS.” *YouTube*, YouTube, 11 Oct. 2021, www.youtube.com/watch?v=o_g-M7UBqI8.

[2]“Quantum Attack Resource Estimate: Using Shor’s Algorithm to Break RSA vs DH/DSA vs ECC.” *RSS*, kudelskisecurity.com/research/quantum-attack-resource-estimate-using-shors-algorithm-to-break-rsa-vs-dh-dsa-vs-ecc. Accessed 17 Nov. 2025.

[3]Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pages 175–179. Bangalore, India, 1984

4]T. Schmitt-Manderbach et al. Quantification of the impact of photon distinguishability on... Electronics (MDPI), 7(4):49, 2018. “effective error correction and privacy amplification . . . when the QBER is below 11

[5] Taehyun Kim, Ingo Stork genannt Wersborg, Franco N. C. Wong, and Jeffrey H. Shapiro. Complete physical simulation of the entangling-probe attack on the bb84 protocol. Physical Review A, 75(4):042327, 2007.

[6]Ayan Biswas, Anindya Banerji, Pooja Chandravanshi, Rupesh Kumar, and Ravindra P. Singh. Experimental side channel analysis of BB84 Qkd source. IEEE Journal of Quantum Electronics, 57(6):8000207, 2021

[7] Zhan, T., Li, H., Huang, P., Chen, H., Han, J., Wu, Z., Fang, H., Yin, H., Zhou, Z., Fu, H., Ji, F., Tan, P., Zhou, Y., Jiang, X., Wang, T., Wu, J., Ye, C., Miao, Y., Qi, W., & Zeng, G. (2025). *Long-distance free-space quantum key distribution with continuous variables*. arXiv preprint arXiv:2507.21546 [quant-ph]

[8] Popa, A.-B. & Popescu, P. G. (2024). *The future of QKD networks*. arXiv:2407.00877.

Entangled Probe Back Up

$$U\big(|\uparrow_z\rangle \otimes |e_0\rangle\big) = |\uparrow_z\rangle \otimes |e_\uparrow\rangle,$$
$$U\big(|\downarrow_z\rangle \otimes |e_0\rangle\big) = |\downarrow_z\rangle \otimes |e_\downarrow\rangle,$$

$$|\uparrow_x\rangle = \tfrac{1}{\sqrt{2}}\big(|\uparrow_z\rangle + |\downarrow_z\rangle\big)$$

$$\Rightarrow\ U\big(|\uparrow_x\rangle \otimes |e_0\rangle\big) = \tfrac{1}{\sqrt{2}}\big(U|\uparrow_z\rangle \otimes |e_0\rangle + U|\downarrow_z\rangle \otimes |e_0\rangle\big)$$
$$= \tfrac{1}{\sqrt{2}}\big(|\uparrow_z\rangle \otimes |e_\uparrow\rangle + |\downarrow_z\rangle \otimes |e_\downarrow\rangle\big)$$

Use $|\uparrow_z\rangle = \frac{1}{\sqrt{2}}(|\uparrow_x\rangle + |\downarrow_x\rangle)$, $|\downarrow_z\rangle = \frac{1}{\sqrt{2}}(|\uparrow_x\rangle - |\downarrow_x\rangle)$

$$\Rightarrow\ U\big(|\uparrow_x\rangle \otimes |e_0\rangle\big) = \tfrac{1}{\sqrt{2}} \cdot \tfrac{1}{\sqrt{2}}\Big((|\uparrow_x\rangle + |\downarrow_x\rangle) \otimes |e_\uparrow\rangle + (|\uparrow_x\rangle - |\downarrow_x\rangle) \otimes |e_\downarrow\rangle\Big)$$
$$= \tfrac{1}{2}\Big(|\uparrow_x\rangle \otimes \big(|e_\uparrow\rangle + |e_\downarrow\rangle\big) + |\downarrow_x\rangle \otimes \big(|e_\uparrow\rangle - |e_\downarrow\rangle\big)\Big)$$

Probability of obtaining $|\downarrow_x\rangle$ (error) when $|\uparrow_x\rangle$ prepared:

$$P_{\text{err}|X} = \left\| \tfrac{1}{2}\big(|e_\uparrow\rangle - |e_\downarrow\rangle\big) \right\|^2 = \tfrac{1}{4}\langle e_\uparrow - e_\downarrow \,|\, e_\uparrow - e_\downarrow\rangle$$

$$= \tfrac{1}{4}\big(\langle e_\uparrow|e_\uparrow\rangle + \langle e_\downarrow|e_\downarrow\rangle - \langle e_\uparrow|e_\downarrow\rangle - \langle e_\downarrow|e_\uparrow\rangle\big)$$
$$\big(\text{assume } \langle e_\uparrow|e_\uparrow\rangle = \langle e_\downarrow|e_\downarrow\rangle = 1\big)$$

$$= \tfrac{1}{4}\big(2 - \langle e_\uparrow|e_\downarrow\rangle - \langle e_\downarrow|e_\uparrow\rangle\big) = \tfrac{1}{4}\big(2 - 2\,\text{Re}\langle e_\uparrow|e_\downarrow\rangle\big)$$

$$= \tfrac{1}{2}\big(1 - \text{Re}\langle e_\uparrow|e_\downarrow\rangle\big)$$

Unitary Operator

- A unitary operator is a reversible, probability-preserving evolution; in the entangling probe model it lets the eavesdropper create correlations with the signal without measuring or cloning it, with the amount of disturbance determined entirely by how distinguishable the probe states become under this unitary
- Common optical components implement unitaries, demonstrating that such interactions are not just theoretical although my example was idealized for simplicity
- Beam splitters implement unitary interactions: they mix two optical modes of photons via a reversible, probability-preserving unitary transformation.

$$U^\dagger U = U U^\dagger = 1$$